Published and Copyright (c) 1999 - 2010
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat
Uwe Seimet

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

~ Avoiding Haiti Scams! ~ People Are Talking! ~ HDDriver Forum Open!
~ More Net Neutrality BS ~ USB 3.0 Finally Here! ~ Conficker Still Here!

~ iTablet Scavenger Hunt ~ Cerny Gets the Call! ~ Call of Duty: Billion!
~ Proof of the iTablet? ~ Donate to Haiti Funds! ~ Duke Nukem Forever?

-* FBI Warns of Bad Haiti Scams *-
-* IE Flaw Allows China Google Attack? *-
-* US, Google, and China in Internet Squabble *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

It's been another one of those long weeks here. And, as usual, I'm tired. But, that's nothing compared to what the people of Haiti have been facing the past few days. A part of a impoverished nation has been destroyed by a devastating earthquake. They need help, so if you can send a little something to help in the rescue and relief effort, please do so quickly. It's that simple. Anything else that I could be writing about this week would only pale in comparison to this disaster, so I'm not going to add any other comments this week.

Until

=~=~=~=

The Official HDDRIVER Forum Is Now Open

Hi!

In order to extend the support for HDDRIVER there is now a special forum for HDDRIVER-related issues: http://www.seimet.de/atari/forum/.
This forum will provide news and first-hand information on anything concerning HDDRIVER and the tools included in the HDDRIVER distribution.

Best regards

Uwe

Dr. Uwe Seimet
http://www.linkbylink.net/

=~=~=~=

PEOPLE ARE TALKING
compiled by Joe Mirando

joe@atarinews.org

Hidi ho friends and neighbors. Okay, let’s get it out of the way right at the top, shall we?

Haiti.

What else is there to say? By now, unless you’ve been living in a cave with no modern media of any kind (in which case you wouldn’t be reading this either), you’ve heard about the earthquake that hit Haiti. Yeah, it is a catastrophe in the true sense of the word. No, it wasn’t the biggest earthquake ever recorded, but pretty darned big, and certainly bigger than the buildings in Port-au-Prince were built to withstand.

And yeah, the devastation there is terrible. The lack of building codes made it worse, of course, but let’s face it, this earthquake was going to cause damage no matter what.

The toll in material things is going to be huge, but even that will be dwarfed by the human cost. In a country where half the population doesn’t have running water and lives on less than a dollar a day, ANY added turmoil is an extreme hardship.

And the hell of it is that the past several years have seen a fairly stable Haiti. Political turmoil has been at a minimum. That is going to change now, mark my words. People are going to lose patience and are going to start "looking out for number one". It’s human nature when faced with disaster.

I want to move on to other things, but let me finish up with saying that the Haiti just can’t seem to get a fair shake. Even in the movie Pirates of the Caribbean... remember the port of Tortuga? That’s the little island just off the coast up above Haiti... it seems it’s always been a place of that’s had problems. From pirates to tin-pot despots and now natural catastrophe, it seems that this little island nation just can’t catch a break.

I won’t belabor the thought, but seriously consider donating to the Red Cross or any other org that’s helping out. Or you can help those who are helping... I’m sure that the Fairfax, VA fire department (one of the first on the ground in Haiti after the quake) would appreciate a little bit of a donation to defray costs.

Also, if you KNOW somebody in Haiti and want to send something to them, consider using UPS... UPS announced the other day that anything that goes to Haiti goes for free until things get going again... I don’t have any details, but an official UPS shipper should be able to give you info on it.

But that’s not the end of it. Now take the money that it would have cost you to ship whatever it is and DONATE that to the Red Cross or to any org that’s helping out. Come on. You can afford that. We’re not talking about a lot of money. Do it just because you CAN. THERE. How’s THAT for paying it forward?

Okay. On to the other topic I want to touch on: Google vs. the Great FireWall of China.

This past week, Google announced that some gmail accounts in China had been... and I love this phrasing... ’compromised’. We’re talking not only about corporate-type accounts, but also the accounts of Chinese civil rights activists.

That’s nothing new. There have been attacks of all sorts coming out of China for several years now. What IS different is that Google is now taking a stand. Evidently, they’re ready to take a stand and say "Y’know what, China? We’re not going to censor stuff the way you want anymore."

Of course, China will then block all kinds of stuff, basically punishing not only it’s own citizens, but Google as well.

This is bad stuff no matter who you are, and I don’t think that anyone other than Google has realized exactly why just yet.

Think about it.. if China can do it, so can about 200,000 other countries, companies and organizations around the world. It’s not just Chinese dissidents that are at risk. Its anyone who assumes they have any expectation of privacy. China is a monster organization; a behemoth of malice and restriction and suppression. That’s how it maintains its existence. And like any organization, the bigger it is, the more desperate it becomes to continue its own existence at the cost of anything else.

Google? Well, it’s the same thing with Google without the tanks rolling through the square to squash some college student. They have softer, gentler means. I’m not saying that they are the technological equivalent to China. Not by any means. But an organization will act like a living organism to maintain its own existence. Fortunately, Google is, for now, much more beneficent and benign than the most populace country in the world. I mean, their motto IS "Don’t Be Evil", after all, isn’t it? [grin]

But there are some new developments in this thing that you may well have heard about by now, but they’re brand new to me at the time of this writing... things like China reminding Google... gently, of course... that they must obey Chinese laws while operating in China.

Google.cn has since lifted censorship and, by the time you read this, they may have clamped down again, or they may be blocked completely by the government.

It also looks like hacking these accounts was part of a much broader effort on the part of the Chinese government... part of a wide system of corporate and political espionage. Something that’s been going on for years. Did China just make the mistake of messin’ with the baddest dude on the block? Is Google going to risk walking away from the fastest growing and possibly largest potential audience in the entire world? Would Ask or Yahoo! or Bing do the same? Would Google assume that they would?

And shortly after Google stopped censoring results and the government warned them about following existing laws, ’researchers’ have identified the IPs used in some of the attacks... yeah, they originated in China. No big news there. But I wonder if there could possibly be someone else involved. Someone intent on making use of China’s reputation in the computing world and world of politics, and able mount a coordinated attack and making it look like it was the work of the Chinese government. Does anybody ELSE remember SPECTRE from the James Bond novels? C’mon, people.

Of course, it could simply be, as I believe it is, that China IS SPECTRE.

But I do have one last, final (for now) thought. What if they have a 'partner'... After all, we now know that most of these intrusions were carried out using a flaw in Internet Explorer.. the "0-Day Flaw". And, of course, Microsoft has been very slow to do anything about a lot of the security flaws in Internet Explorer. Could it possibly be that they...

Nahhhhhh... I've been reading too many espionage novels. [grin]

Well folks, that's it for this time around. Tune in again next week, same time, same station, and be ready to listen to what they are saying when [shhhh! The Chinese government might hear us!]...

People Are Talking

[Editor's note: Sorry folks. It turns out that the "UPS ships free to Haiti" thing is a hoax. Dammit.
See: http://www.snopes.com/inboxer/charity/haiti.asp

But on the up-side, UP side, UPS is donating a million dollars to the relief effort. Here's their blog entry on the subject:

But that doesn't mean you can't donate. Remember: UPS can give a million dollars, and that's great!.. but if two million of us give a buck each, we've got 'em beat by a country mile. Let's pitch in and do a little bit of good, huh?

Thanks again, and see ya next week,

Joe

=~=~=~=

->In This Week's Gaming Section - 'Call of Duty' Makes $1 Billion!
""""""""""""""""""""""""""""""""" Duke Nukem Forever To Be Released?
Mark Cerny Into Hall Of Fame!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""

Activision Blizzard: 'Call of Duty' Has Made $1 Billion

Video game publisher Activision Blizzard Inc. said Wednesday that the game "Call of Duty: Modern Warfare 2" has brought in more than $1 billion in revenue since it went on sale in November.

Given that pace, the game is on track to become the best selling video game ever by number of copies sold, said Michael Pachter, an analyst at Wedbush Morgan.

Based on the revenue figure, Pachter said the company has probably shipped about 17 million copies of the game so far. And he expects it to surpass the roughly 23 million copies sold of "Grand Theft Auto: San Andreas," which was released in 2004 and holds the previous record.

"Call of Duty" has an edge because of its online multi-player mode. New updates to the online version can give titles a longer shelf life.

Still, Pachter said he doesn't expect Activision's fourth-quarter financial results to surpass expectations. "They're not killing it, but they're making it," he said.

While "Call of Duty" sales are "impressive," titles such as "Guitar Hero" have been lackluster.

Others in the video game industry have given indications of weak holiday sales. Rival Electronic Arts Inc. this week slashed its 2009 earnings estimate for the second time. GameStop Corp., the world's biggest video game retailer, said sales during the shopping season dropped 8.6 percent from the year before.

Duke Nukem Actor Hints that Duke Nukem Forever Will be Released

The voice of Duke Nukem has apparently rekindled hope among fans that the stuck-in-limbo Duke Nukem Forever may yet see the light of day. Actor Jon St. John spoke during a panel at the recent Music and Games Festival held in Alexandria, Virginia, where he responded to a question from a fan about the status of 3DRealm's sordid affair. According to Pixel Enemy the actor said the following:

"I'm not allowed to speak on that subject, sir. He's asking about Duke Nukem Forever, let me go ahead and tell you right now that I'm not allowed to talk about Dukem Nukem Forever.

No, no, don't be disappointed, read between the lines... why am I not allowed to talk about it?"

Clearly hinting that Duke Nukem Forever will eventually see the light of day, St. John's comment backs up 3DRealms' Scott Miller's claim from last month, which suggested that development of the project is still ongoing. To be continued...

Gran Turismo 5 Delayed Indefinitely

In a surprise press statement, Sony today revealed its much anticipated uber-racer Gran Turismo 5 for the PlayStation 3 has been delayed with a new release date as yet unsettled. The game had been due in Japan this

March, with a US and European release date targeting summer 2010.

'To Be Announced', that's the racer's new status, and while Sony isn't saying why the game's been delayed, they are apologizing for the unanticipated hangup.

If you've followed the game, you know it's been in development forever, that it's cost incredible sums (the game's 'godfather' Kazunori Yamauchi put the figure at $60 million as of last November), that it's supposed to be breathtakingly realistic with 1,000 cars and over 20 track locales, and that the skeletal prologue version released over two year ago has itself sold around 3.5 million copies to date.

Sony told game news site CVG that GT5's delay applies to the Japanese market alone. Japan's the only territory where the game had received a firm release date.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

AIAS To Induct Mark Cerny Into Hall Of Fame

The Academy of Interactive Arts & Sciences will honor legendary game developer Mark Cerny with an induction into its Hall of Fame alongside luminaries such as Shigeru Miyamoto, Sid Meier, John Carmack, and Will Wright.

Cerny, a 25-year programming and design veteran, first gained fame for his 1984 hit Marble Madness while working at Atari. Throughout the 1990s and 2000s he worked extensively with Los Angeles-area PlayStation developers Naughty Dog and Insomniac Games, proving crucial to the early success of those studios. More recently he has worked with Sony's internal core development group, Ice Team.

"I'm thrilled to accept this award, which clearly has a lot to do with the drive and talent of the many teams that I've had the pleasure to work with over the years," he said in response to the announcement.

"Mark Cerny is the closest we have come to a modern-day Da Vinci," said AIAS president Joseph Olin in a statement. "What he does isn t restricted to a single aspect of game creation, he really is a Renaissance man."

"He is a diversely accomplished game designer, producer, programmer and technologist, fluent in Japanese and one of the foremost Western experts on the Japanese game market. He s also one of the only top-level independents in a business dominated by institutions."

"Mark is one of the only individuals who have managed to stay on the cutting edge of game development from the heyday of arcade games all the way up to the current generation of gaming consoles. Each step of the way he's redefined how the industry thinks about game design, technology, and

production philosophies," said Naughty Dog co-president Evan Wells.

Cerny also received the similar Lifetime Achievement Award at 2004's Game Developers Choice Awards. He joins Wright, Miyamoto, Meier, and Carmack as overlapping recipients of both honors.

He will be formally inducted during the AIAS' award show held during the DICE Summit in Las Vegas this February.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

U.S., Google and China Square Off over Internet

Google's threat to quit China over censorship and hacking intensified Sino-U.S. frictions on Wednesday as Washington said it had serious concerns and demanded an explanation from Beijing.

China has not made any significant comment since Google, the world's top search engine, said it will not abide by censorship and may shut its Chinese-language google.cn website because of attacks from China on human rights activists using its Gmail service and on dozens of companies, including Adobe Systems.

"Google's action should be a wake-up call to everyone involved in China's economy - U.S. businesses, the U.S. administration and the Chinese themselves," said Tony Fratto of the Hamilton Place Strategies consulting firm.

Media freedom groups who had severely criticized Google's previous compliance with Chinese curbs praised the company's decision and called for other firms to follow suit.

"A foreign IT company has finally accepted its responsibilities toward Chinese users and is standing up to the Chinese authorities, who keep clamping down more and more on the Internet," said Reporters Without Borders.

However, investors were spooked and U.S. and Chinese analysts warned of turbulent bilateral ties in 2010.

Technology business analysts noted in reports issued on Wednesday that Google draws $300-600 million in revenue from China - less than 5 percent of its sales. But they voiced concerns about Google's future prospects in that huge market.

Friction over the Internet, part of a long-running dispute over human rights, appears likely to stoke U.S.-China tensions. Analysts predicted clashes on climate change, China's crackdown on dissidents, Iran's nuclear ambitions and other issues.

President Barack Obama’s administration, which in 2009 strived to embrace China as a partner in tackling global issues, has angered China by approving arms sales to Taiwan and by slapping tariffs on Chinese tires and steel products.

Obama is also expected to meet with the Dalai Lama of Tibet, a world religious figure whom China reviles and accuses of leading a Tibetan separatist drive. Obama avoided meeting the exiled Tibetan leader last year to pave the way for a summit with Chinese President Hu Jintao in November.

Writing before the Google decision, The Eurasia Group consultancy said looming economic friction made U.S.-China relations the top global risk of 2010.

"In the future, we’ll look back at that summit as the peak of the relationship, and we’ll see significant deterioration in U.S.-Chinese relations in the coming year," the group wrote.

White House spokesman Robert Gibbs sidestepped questions about the possible impact on U.S.-China relations and said Washington awaited an explanation from China on the attacks.

"The president and this administration have beliefs about freedom of the Internet," he said.

Chinese authorities were "seeking more information on Google’s statement," the Xinhua news agency reported, citing an unnamed official from China’s State Council Information Office, the government arm of the country’s propaganda system.

Admiral Robert Willard, head of the U.S. Pacific Command, told a congressional hearing that "U.S. military and government networks and computer systems continue to be the target of intrusions" that appear to have originated from China.

While most cyber-attacks focus on prying out data, "the skills being demonstrated would also apply to wartime computer network attacks," he said.

Sen. Joe Lieberman, chairman of the Senate Homeland Security and Governmental Affairs Committee, said he was drafting legislation to strengthen U.S. cyber security.

"Google’s experience should be a lesson to us all to confront this ever growing problem aggressively and with all available means," he said in a statement.

China has said it does not sponsor hacking.

Pressing China for an explanation, U.S. Secretary of State Hillary Clinton said: "The ability to operate with confidence in cyberspace is critical in a modern society and economy.

With China the largest lender to the United States, holding $800 billion in Treasury bills, Internet tensions will make steering this vast, fast-evolving relationship all the more tricky, especially with the U.S. Congress in an election year.

"China has been taking a harder line," said Shi Yinhong, an expert on relations with the United States at Renmin University in Beijing. "The next few months are going to see some turbulence in China-U.S. relations. We may see some tactical concessions from China, but the general trend isn't toward compromise."

Chinese industry analysts said the issue had snowballed beyond Google.

"If this becomes heavily politicized, and there are signs that it is, and people in the Chinese government say, 'This is good. It serves you right, and we won't bow our heads to the United States,' then there'll be no way out," said Xie Wen, a former executive in China for Yahoo and other big Internet companies, who is now an industry commentator.

"The impact on China's image will gradually also affect the enthusiasm of investors," he added. "It's not the pure economic losses - a billion or so - it's the deteriorating environment."

China's policy of filtering and restricting access to Web sites has been a frequent source of tension with the United States and tech companies, such as Google and Yahoo Inc.

Google's announcement suggested the recent intrusions were more than isolated hacker attacks.

"These attacks and the surveillance they have uncovered -- combined with the attempts over the past year to further limit free speech on the Web -- have led us to conclude that we should review the feasibility of our business operations in China," Google's chief legal officer David Drummond said in a statement posted on the company's blog.

Some 20 other companies also were attacked by unknown assailants based in China, said Google.

Google's potential withdrawal from China shocked investors and analysts, who fear the web search leader's strategic plans may be threatened.

"For investors this is clearly a negative," Broadpoint AmTech analyst Benjamin Schachter said in a research note. "The obvious concern is that China's growth has been solid and its market potential is enormous."

Such concerns pushed investors toward Chinese search engine Baidu Inc, which leads Google in China's search market with more than 60 percent share. Shares of Baidu jumped 12 percent to $432 in early trading, while Google shares slipped 2 percent to $579.

Obama, during a visit to China in November, told an online town hall that he was "a big supporter of non-censorship."

After the Google announcement, searches on its google.cn search engine turned up images and sites previously blocked, including pictures from the 1989 crackdown on pro-democracy protests in Beijing. Other searches remained restricted, carrying messages warning users that some content was blocked.

China's ruling Communist Party, wary of the Internet becoming an uncontrolled forum for the country's 360 million Internet users, is unlikely to allow Google to avoid repercussions.

If google.cn, launched in 2006, shuts down, Beijing could seek to

restrict access to Google’s main search engine, which can also do searches in Chinese, although China’s "firewall" of filters blocks many users from opening up the results.

"The general tendency over the past year has been to accuse foreigners of having a Cold War mentality and being anti-China," said Rebecca MacKinnon, an expert on the Chinese Internet at the Open Society Institute.

"How exactly they are going to react to this, I cannot anticipate, but it’s likely that it will not be pretty."

IE Exploit Used to Launch Chinese Attacks on Google

Early speculation focused on the Abobe Reader zero-day exploit as the source of the Chinese attacks on Google and other corporations earlier this week, but Adobe may be off the hook - or at least share the blame. Microsoft has determined that an unknown flaw in Internet Explorer was one of the holes used to launch the attacks which have led to Google threatening to shut down its Chinese operations.

Microsoft Security Response Center director Mike Reavey said in an e-mailed statement "This afternoon, Microsoft issued Security Advisory 979352 to help customers mitigate a Remote Code Execution (RCE) vulnerability in Internet Explorer. The company has determined that Internet Explorer was one of the vectors used in targeted and sophisticated attacks targeted against Google and other corporate networks."

Reavey continued "Microsoft continues to work with Google, other industry partners and authorities to actively investigate this issue. To date, Microsoft has not seen widespread customer impact, rather only targeted and limited attacks exploiting IE 6."

The revelation of the zero-day bug in Internet Explorer, and the release of the security advisory from Microsoft, comes just two days after Microsoft’s regularly scheduled Patch Tuesday for the month of January. Coincidentally, Adobe also issued a security update this past Tuesday which addresses the zero-day flaw in Adobe Reader that has been exploited in-the-wild since at least mid-December.

Microsoft is continuing to investigate the issue, and no patch or update has yet been issued, but the security advisory from Microsoft does contain some mitigating factors you can focus on to protect your PC’s from this flaw in the meantime:

* Protected Mode in IE7 on Windows Vista limits the impact of the vulnerability.

* In a Web-based attack scenario, an attacker could host a webpage that is used to exploit this vulnerability or do so via a webpage that accepts or hosts user-provided content or advertisements. In all cases, however, an attacker would have no way to force users to visit these websites and would have to convince them to do so, which is typically achieved via an e-mail or instant message.

* By default, Internet Explorer on Windows Server 2003 and Windows

Server 2008 runs in a restricted mode that is known as Enhanced Security Configuration. This mode sets the security level for the Internet zone to High and so is a mitigating factor for websites that you have not added to the Internet Explorer Trusted sites zone.

* An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

* By default, all supported versions of Outlook, Outlook Express, and Windows Mail open HTML e-mail messages in the Restricted sites zone, which should mitigate attacks trying to exploit this vulnerability by preventing Active Scripting and ActiveX controls from being used. However, if a user clicks a link in an e-mail message, the user could still be vulnerable to exploitation of this vulnerability through the Web-based attack scenario.

"It could also be possible to display specially crafted Web content using banner advertisements or other methods to deliver Web content to affected systems. The Microsoft investigation concluded that setting the Internet zone security setting to "high" will protect users from the vulnerability addressed in this advisory," added Reavey.

There is no indication from Microsoft yet about whether we should expect an out-of-band patch to address this issue before the next regularly-scheduled Patch Tuesday, but I wouldn’t be surprised. Take a look at the security advisory and take the appropriate steps to protect your PC’s from the Internet Explorer vulnerability. You should also apply the Adobe security update to protect your systems from the Adobe Reader zero-day exploit.

FBI Warns of Bogus Haiti Online Donation Scams

The U.S. Federal Bureau of Investigation is advising people to be careful when evaluating donation programs related to the earthquake in Haiti as one security firm is already seeing scam e-mails circulate.

People should apply a "critical eye" to requests for financial donations following Tuesday’s earthquake in Haiti, which caused an unknown number of deaths and severe damage to the country’s infrastructure.

"Make contributions directly to known organizations rather than relying on others to make the donation on your behalf to ensure contributions are received and used for intended purposes," the FBI said in its advisory.

Scam e-mails are already emerging. Symantec noted a so-called 419-style e-mail that purported to come from the British Red Cross. A 419 scam, named after the number of a statute in Nigeria’s criminal code banning the practice, is one in which an e-mail or a letter implores a person to send money for some bogus reason.

Although most people dismiss the appeals, people still do fall for them, especially when they’re linked to events such as a natural disaster.

The fake British Red Cross e-mail uses the real London address of the

organization, according to Mathew Nisbet, a malware data analyst with Symantec Hosted Services. The contact e-mail for the British Red Cross is wrong, however, and the organization doesn't collect donations using the Western Union money transfer service, either.

"Any money sent using the instructions in this e-mail would not help anyone in Haiti," Nisbet wrote. "It would end up in the pockets of a cybercriminal."

Other cybercriminals are using the tragedy in Haiti as part of a hook to trick people into visiting other harmful Web sites seeded with fake antivirus applications, according to another security vendor, Websense.

The scammers build a shell of a Web site loaded with, for example, information that purports to relate to the earthquake in Haiti. Using techniques generally banned by various search engines, the scammers are able to get their Web site returned on the first page of results when someone does a search.

Websense researchers show in a video on their blog that, at one point since the tragedy happened, typing "Haiti relief" in Google turned up some of those sites.

When clicked, the sites redirect to other sites hosting fake antivirus programs. Deceptive means are used to trick people into installing the applications. Also, security vulnerabilities can be exploited in order to install the programs. The programs then display pop-up messages and warnings in order to goad users into paying for the programs.

The fake antivirus application scam has become widely prevalent. Security vendor PandaLabs estimated last year that 35 million computers worldwide were infected with those kinds of programs per month.

How to Avoid Haiti Quake Scams

When a major disaster like the quake in Haiti hits, good people and groups around the world step up to offer help and donations. Right behind them evil scammers around the world scramble to intercept those donations. In the next few days you'll probably encounter numerous e-mails, Facebook groups, and tweets with links to sites requesting donations to help the quake victims. How can you separate the valid charities from the frauds?

Here are ten tips to ensure your donations go to the right place.

1. *Sanity-check URLs*. Some scammers are sloppy. If an e-mail message claims to be from the International Red Cross, say, but the URL links point to something wildly different, stay away! Not sure? In most e-mail clients you can point to a link with the mouse and see the actual URL in the status bar or in a tooltip.
2. *Decode Short URLs*. If a tweet or other post includes a shortened URL pointing to a charity site, don't click it. Instead, use one of the many services that retrieve the full URL. Here again, if it looks wrong, stay away.
3. *Don't Even Click Valid URLs*. Even if the links in an e-mail appear to be valid, don't click them. Instead, navigate directly to the organization's web site and look for information about

helping disaster victims.

4. *Run a Background Check*. We can’t all be familiar with every legitimate aid group. Before visiting a group you don’t recognize, check the site’s ownership using www.whois.net or another site that supplies whois data. This should give you the full company name, an address, a contact name, and a phone number. If the results don’t jibe with the stated name, stay away.
5. *Do a History Check*. You’ll surely feel safer donating to a charity Web site that’s been around for a while. Go to the Internet Archive and check the site’s history. If there’s no history, the site is very recent. Yes, it could be that the organization was formed to help with the current crisis, but it could also point to an opportunistic scam.
6. *Ask the Better Business Bureau*. The Better Business Bureau online offers a page that lets you check their charity reviews. You can search by name, URL, e-mail address or phone number. A positive response means it’s a valid charity, but "not found" isn’t necessarily a black mark. For example www.icrc.org, the Web site for the International Committee of the Red Cross, isn’t in the BBB database.
7. *Don’t Donate Cash*. If the charity asks for cash, offers to send a messenger to pick up your donation, pressures you to donate more than you’ve offered, or otherwise seems over-eager, disengage right away. Your safest donation is a check, made out to the organization and not to any individual.
8. *Beware Collateral Damage*. Scammers trolling for cash aren’t your only worry. As with other newsworthy search terms, searches about the Haiti quake may turn up malicious Web sites. The bad guys get these sites into search results using what’s called "SEO poisoning" (SEO means Search Engine Optimization). Click the wrong one and you may be hit with a drive-by download; let’s hope your security suite blocks it.
9. *Give to Groups*. You may get an appeal through e-mail or social networking from an unfamiliar individual claiming to be a victim and asking for your direct help. It may seem hard-hearted, but don’t respond. Impersonating a victim is much easier than impersonating a charity. If the appeal touches your heart, make your donation to a known aid organization.
10. *Give Proactively*. Supposing you do want to donate money toward aiding the quake victims, don’t wait for an invitation. Locate a likely charity that’s helping in that area and contact them to make your donation. Now you can ignore any other possibly-unsafe requests for donations with a clear conscience.

Of course these tips aren’t limited to the Haiti quake. You should take care whenever responding to requests for help, or to any unsolicited e-mail or social networking contact. That way your help will go to those who need it, not to the vultures.

Court Questions FCC Authority to Impose Net Neutrality

No decision has been made yet, but, if Friday’s arguments before the U.S. Court of Appeals in DC are any indication, it doesn’t appear that the FCC will prevail in exerting its authority over Comcast. Losing this battle may be just what the FCC needs to move forward with its efforts to formalize net neutrality guidelines.

The case before the court is an appeal from Comcast related to sanctions imposed on it by the FCC for discriminating against peer-to-peer networking file traffic in an effort to throttle bandwidth demand on its broadband network. Comcast's challenge claims the FCC has no such authority.

FCC chairman Julius Genachowski has stated that the FCC acted based on the Four Freedoms outlined by the previous FCC administration in 2005. These principles, while not formal rules, have been used to govern net neutrality on a case-by-case basis:

* 1. Consumers are entitled to access the lawful Internet content of their choice.
* 2. Consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement.

* 3. Consumers are entitled to connect their choice of legal devices that do not harm the network.

* 4. Consumers are entitled to competition among network providers, application and service providers, and content providers.

The crux of the FCC sanctions lies with the first and second principles. However, the caveats of "subject to the needs of law enforcement" and "that do not harm the network" provide ample latitude for providers to act to restrict certain activities or types of network traffic.

The Comcast appeal claims "There was simply no federal law to interpret, enforce, or apply against Comcast" in challenging the FCC authority, and the three-judge panel of the appeals court appears to agree with that assertion.

The reality is that Comcast, and the appeals court if it ultimately sides with Comcast, have a valid point. While the Four Freedoms were established and documented, they represent more of a general framework rather than established rules. The fact is that the FCC does not have formal net neutrality rules in place and its authority to implement them is up for debate.

Based on how the case is proceeding now, it seems obvious that the appeals court will decide in favor of Comcast, leading to misguided speculation that the case will validate opposition to the FCC authority over Internet providers and put a nail in the coffin of its efforts at establishing formal net neutrality rules.

On the contrary, losing this case could provide the impetus to more formally define the FCC authority over Internet providers, and provide momentum to push through the net neutrality rules. The FCC is fortunate that the court makes decisions based on established rules and precedent, but it does not make policy or have any authority itself to define or restrict the scope of the FCC.

If, in fact, Comcast wins its appeal based on the fact that the Four Freedoms are merely a loose set of principles rather than a formalized regulatory framework, it underscores the importance of creating such a framework.

Losing this court case will provide the FCC with tangible proof for why the pursuit of net neutrality is so urgent, and give Congress incentive to more clearly specify the scope of the FCC's authority to oversee and

police wired and wireless broadband providers.

Comcast prevailing in this appeal could be just the incentive needed to drive FCC efforts to develop formal net neutrality rules.

Conficker Worm Hasn’t Gone Away, Akamai Says

Variants of the Conficker worm were still active and spreading during the third quarter, accounting for much of attack traffic on the Internet, according to Akamai Technologies.

"Although mainstream and industry media coverage of the Conficker worm and its variants has dropped significantly since peaking in the second quarter, it is clear from this data that the worm (and its variants) is apparently still quite active, searching out new systems to infect," Akamai said in its State of the Internet report for the third quarter of 2009, released Thursday.

During the third quarter, 78 percent of Internet attacks observed by Akamai targeted port 445, up from 68 percent during the previous quarter. Port 445, which is used by Microsoft Directory Services, is the same port that Conficker targets, aiming to exploit a buffer overflow vulnerability in Windows and infect the targeted computer.

Most attacks originated from Russia and Brazil, which replaced China and the U.S., as the top two sources of attack traffic. Russia and Brazil accounted for 13 percent and 8.6 percent of attack traffic, respectively, Akamai said. The U.S., which came in at No. 3, accounted for 6.9 percent of attack traffic and No. 4 China accounted for 6.5 percent, it said.

"Port 445 was overwhelmingly the top port targeted by attacks originating in Russia and Brazil, which may indicate the presence of a large number of systems in both countries actively participating in Conficker-related botnets," Akamai said.

While Microsoft has issued a patch that fixes the vulnerability exploited by earlier versions of Conficker, experts believes the worm remains active because many infected machines are running unlicensed copies of Windows and don’t have access to security updates.

Citing figures from the Conficker Working Group, Akamai noted that the number of Conficker.A and Conficker.B infections worldwide rose during the third quarter, while infections of Conficker.C declined during the same period.

However, recent numbers estimates for the number of Conficker infections appear to have moderated somewhat, with the number of computers infected with Conficker.A or Conficker.B dropping from a high of around 6.7 million in late October to around 6.3 million machines today.

The number of Conficker.C infections has declined from 400,000 computers in late October to roughly 280,000 today.

USB 3.0 Finally Arrives

When you’re in front of your PC, waiting for something to trans fer to removable media, that’s when seconds feel like minutes, and minutes feel like hours. And data storage scenarios such as that one is where the new SuperSpeed USB 3.0’s greatest impact will be felt first. As of CES, 17 SuperSpeed USB 3.0-certified products were introduced, including host controllers, adapter cards, motherboards, and hard drives (but no other consumer electronics devices). Still more uncertified USB 3.0 products are on the way, and they can’t get here fast enough.

The beauty of USB 3.0 is its backward compatibility with USB 2.0; you need a new cable and new host adapter (or, one of the Asus or Gigabyte motherboards that supports USB 3.0) to achieve USB 3.0, but you can still use the device on a USB 2.0 port and achieve typical USB 2.0 performance. In reducing some overhead requirements of USB (now, the interface only transmits data to the link and device that need it, so devices can go into low power state when not needed), the new incarnation now uses one-third the power of USB 2.0.

The theoretical throughput improvement offered by USB 3.0 is dramatic - a theoretical 10X jump over existing USB 2.0 hardware. USB 2.0 maxed out at a theoretical 480Mbps, while USB 3.0 can theoretically handle up to 5Gbps. Mind you, applications like storage will still be limited by the type of drive inside; so, for example, you can expect better performance from RAIDed hard drives or fast solid-state drives (SSDs) than from, say, a standalone single drive connected to the computer via USB 3.0.

The real-world examples are fairly convincing - and underscore USB 3.0’s advantage for high-def video, music, and digital imaging applications. Our early test results are encouraging as well: We tested Western Digital’s My Book 3.0, the first USB 3.0-certified external hard drive. The performance was on a par with that of eSATA-but the benefit here is that USB 3.0 is a powered port, so you don’t need to have another external power supply running to the drive (as you do with eSATA; unless the eSATA drive you’re using is designed to steal power from a USB port while transferring data over the eSATA interface).

While the WD drive was the first to announce, a slew of other hard drive makers either announced products at the show, or discussed plans to release products in the coming months. Among them: Seagate (which is doing a portable drive), LaCie, Rocstor, and Iomega. Even non-traditional hard drive vendors like Dane-Elec and A-Data showed products they billed as USB 3.0 (the latter two even had USB 3.0-connected SSDs, the first external drives to use solid-state storage inside.

One of the things to look for in the coming months is the certified SuperSpeed USB 3.0 logo. Products are currently filling the queues at the official certification testing labs, but presence of that certification logo will give you some peace of mind that the product you’re buying truly does live up to the USB 3.0 spec.

Given that the certification labs are jammed up, though, you can expect companies to release USB 3.0 products without official certification. (Buffalo Technologies’ drive, released late 2009, is not certified; LaCie’s drives are in the process of certification, but will initially carry LaCie’s own logo for USB 3.0, and will gain a sticker on the box once certification is completed.) And in those cases, it will be hard to know whether the device truly lives up to its performance potential.

And this time around, the way the USB spec is written, says Jeff Ravencraft, consumers should have an easier time finding products that are truly USB 3.0. Before, in the transition from USB 1.1 to USB 2.0, the USB 2.0 spec was written in a way where it "encompassed low, full and high-speed USB," explains Ravencraft, president and chairman of the USB Implementers Forum. "Since those are all encapsulated in the USB 2.0 spec, [vendors] could have a certified product that's low-speed, but still call it USB 2.0.

"We don't have that issue with USB 3.0 To claim you're USB 3.0, you have to deliver 5Gbps. There's no other way to get the certification."

Ravencraft adds that the group is prepared to protect the USB 3.0 logo, to make sure that only manufacturers who go through certification use it. "We'll take legal action if anyone infringes on our marks."

By end of year, Ravencraft says the loggerjam of products awaiting certification should be past, and the organization's network of worldwide test labs will be handling USB 3.0 certification.

According to In-Stat Research, by 2013, more than one-quarter of USB 3.0 products will support SuperSpeed USB 3.0.

Ravencraft says this is the fastest ramp up of USB products he's seen in the past ten years, across the previous versions of USB.

I say the change can't come fast enough. The trick, though, will be getting the interface into our notebooks (without requiring a kludgy ExpressCard adapter). So far, though, only HP and Fujitsu have announced limited USB 3.0 support on notebooks. And Taiwanese notebook and desktop maker MSI indicated that it wouldn't have USB 3.0 until, at the earliest, the third-quarter of this year; product managers for both notebooks and desktops cited manufacturing concerns like chipset availability in large quantities, and the need to test USB 3.0 chipsets.

And in the meantime, the only announced peripherals remain storage devices. At next year's CES, it's likely we'll hear more about specific consumer electronics devices such as digital cameras and camcorders and video cameras moving to USB 3.0. Hopefully by then we'll start getting a critical mass of PC hardware with USB 3.0 integrated, too.

iTablet Scavenger Hunt Raises Apple Hackles

A Silicon Valley gossip website has evidently triggered Apple's ire by offering rewards for proof that the notoriously secretive company has made a tablet computer.

Valleywag.com on Wednesday offered 10,000 dollars for "bona fide" pictures of an Apple tablet; 20,000 dollars for video of one in action, and 50,000 dollars if Apple chief executive Steve Jobs was in the pictures or video.

The reward would jump to 100,000 dollars "if you let us play with it for an hour," the website promised while announcing what it dubbed the "Apple Tablet Scavenger Hunt."

By Friday, Valleywag had declared Apple the first winner of its contest due to a letter it said it received from the iconic California company's

lawyers.

"We believe you and your company have crossed the line by offering a bounty for the theft of Apple’s trade secrets," an Apple lawyer said in a copy of the letter posted online by Gawker-owned Valleywag.

"Apple demands that Gawker Media discontinue this program and retract the offer to pay for photos, video, or samples of Apple’s unannounced product."

The Valleywag scavenger hunt was still on Friday, with Gawker warning anyone considering going for the prize not to break the law in the process.

Silicon Valley has been buzzing with rumors that Apple will hold a press event the last week of January to unveil an "iTablet" computer that builds on the popularity of its iPhone and iPod Touch devices.

True to form, Apple has refused to comment on iTablet talk, letting anticipation and speculation build.

The specter of an iTablet hovered over the international Consumer Electronics Show in Las Vegas last week, with manufacturers of tablet computers jockeying for head-starts in the marketplace.

Gag Prize Awarded in Apple Tablet Scavenger Hunt: Proof at Last?

Technology blog Valleywag says it has a winner in its Apple Tablet scavenger hunt offering prizes to anyone who can provide proof the mythical device exists. And the winner is: Apple? That’s right; Gawker Media’s tech blog is awarding a prize to Apple attorney Michael Spillner of the law firm Orrick, Herrington & Sutcliffe for "proving" the existence of Apple’s Tablet. What was the evidence Spillner sent over? A cease-and-desist letter addressed to Valleywag’s Editor-in-Chief demanding an end to the scavenger hunt.

And what was the amazing prize awarded for such a heroic effort? Read on and find out.

On Wednesday, Valleywag promised cash prizes to anyone able to provide authentic photos of the tablet or access to the device itself. Valleywag’s prizes varied depending on the type of evidence provided: $10,000 for actual pictures of the device; $20,000 for a video of the device in action; $50,000 for photos of Steve Jobs holding the tablet; and $100,000 for giving Valleywag one hour of quality time with the device.

Valleywag’s tablet bounty attracted a lot of attention, but many wondered about the legality of the offer since it encourages Apple’s employees and partners to break any non-disclosure agreements they may have signed with Apple. Considering Apple’s penchant for absolute secrecy when it comes to new devices, it’s no surprise the company wanted to end Valleywag’s quest for evidence before things got out of hand.

[Is the] letter from Apple’s attorneys proof positive of the tablet’s existence? Here are the relevant quotes: "I am writing on behalf of Apple regarding the notices...that Gawker Media will pay someone a financial reward for sending you photos, video, or a sample of an unannounced and highly confidential Apple product...The information you are willing to

pay for...constitutes Apple trade secrets...Apple has maintained the types of information and things that you are soliciting...in strict confidence."

On the one hand it's awfully tempting to take this letter at face value, and assume it proves the tablet's existence since the letter refers to "an unannounced and highly confidential Apple product" as if it actually existed.

But then again how could Apple not send this letter? If, as expected, Apple really is making a major product announcement later this month, the company must do everything in its power to stop information leaks. Even if Apple isn't working on a tablet, but some other type of wonder device, there's no way they'd want any information about upcoming devices getting out before a company announcement. So while it makes for an interesting discussion, it's hard to take this letter as proof of anything other than Apple's desire to control access to its intellectual property.

Apple's request gave Valleywag until 6 p.m. Thursday to end the scavenger hunt or risk further legal penalties. So far, Valleywag says the contest is still on.

As for Spillner, Valleywag says he is getting a gift basket for his "entry" that includes a DVD of Legally Blonde 2, one $25 Zune Marketplace giftcard, and a "fabulous set of steak knives."

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.